

**EXHIBIT 4****ISS'S STATEMENT OF ISSUES OF FACT  
THAT REMAIN TO BE LITIGATED**

ISS reserves the right to modify, supplement, or change this Statement of Issues of Fact That Remain to be Litigated (the "Statement") to reflect the Court's rulings on claim construction and the dispositive motions presently pending. ISS also reserves the right to modify, supplement or change this Statement to the extent necessary to fairly respond to any new issues SRI raises in its Statement of Issues of Fact. To the extent that any of these issues is deemed an issue of law rather than an issue of fact, ISS incorporates said issue by reference into ISS's Statement of Issues of Law that Remain to be Litigated. Conversely, to the extent that any issue in ISS's Statement of Issues of Law that Remain to be Litigated is deemed an issue of fact, ISS incorporates said issue by reference into this Statement.

This Statement of Issues of Fact applies only to the liability phase of trial. Issues of damages and willfulness have been bifurcated by the Court and will be addressed separately.

SRI has asserted the following claims against ISS (referred to herein as the "asserted ISS claims"):

<b>Asserted ISS claims</b>	<ul style="list-style-type: none"> <li>• '338 patent: claims 1, 4, 5, 11, 12, 13, 24</li> <li>• '203 patent: claims 1, 2, 4, 6, 12, 13, 15, 17</li> <li>• '615 patent: 1, 2, 4, 13, 14, 16</li> <li>• '212 patent: No claims asserted against ISS's currently accused products. ISS is maintaining its declaratory judgment action of non-infringement and invalidity against claims 1-24 of the '212 patent.</li> </ul>
----------------------------	--

**I. OWNERSHIP**

1. Whether SRI can prove that it has standing to sue as the owner of the '203 patent, the '615 patent, and the '338 patent.

## II. INFRINGEMENT

2. Whether, by a preponderance of the evidence, SRI can prove that RealSecure agents (Network, Guard, Server, and Desktop series) and Proventia agents (A, G, M, Server and Desktop series) when used in combination with the SiteProtector SecurityFusion Module 2.0 (as well as later versions) meets each and every limitation of claims 1, 2, 4, 6, 12, 13, 15, and 17 of the '203 patent and claims 1, 2, 4, 13, 14, and 16 of the '615 patent literally.
3. Whether, by a preponderance of the evidence, SRI can prove that RealSecure agents (Network, Guard, Server, and Desktop series) and Proventia agents (A, G, M, Server and Desktop series) when used in combination with the SiteProtector SecurityFusion Module 2.0 (as well as later versions) meets each and every limitation of claims 1 and 12 of the '203 patent and claims 1 and 13 of the '615 patent with only insubstantial differences.
4. Whether, by a preponderance of the evidence, SRI can prove that ISS has directly infringed the asserted ISS claims of the '203 and the '615 patents in the manner alleged to be infringing.
5. Whether, by a preponderance of the evidence, SRI can prove that any ISS customer has directly infringed the asserted ISS claims of the '203 and '615 patents in the manner alleged to be infringing.
6. Whether, by a preponderance of the evidence, SRI can prove that ISS, with the requisite intent and knowledge, actively induced its customers to infringe the asserted ISS claims of the '203 and '615 patents.<sup>1</sup>
7. Whether, by a preponderance of the evidence, SRI can prove Proventia Network Anomaly Detection System (ADS) operating in standalone mode meets each and every limitation of claims 1, 4, 5, 11, 12, 13, and 24 of the '338 patent literally.
8. Whether, by a preponderance of the evidence, SRI can prove Proventia Network Anomaly Detection System (ADS) operating in standalone mode meets each and every

---

<sup>1</sup> ISS understands that SRI is no longer asserting contributory infringement against any ISS product.

limitation of claims 1 and 24 of the '338 patent with only insubstantial differences.

9. Whether, by a preponderance of the evidence, SRI can prove that ISS has directly infringed the asserted ISS claims of the '338 patent in the manner alleged to be infringing.

### III. INVALIDITY

10. Whether, for each claim, SRI can prove a date of invention earlier than the respective filing date, and such date of invention.

#### A. Anticipation

11. Whether the following printed publications and patents are prior art under 35 U.S.C. § 102(a), (b) or (e):

- P. Porras and A. Valdes, "Live Traffic Analysis of TCP/IP Gateways," (*"Live Traffic"* various versions);
- P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proceedings of the 20<sup>th</sup> National Information Systems Security Conference, pp. 353-365, October 9, 1997 (*"Emerald 1997"*);
- D. Anderson, T. Frivold, and A. Valdes, "Next-generation Intrusion Detection Expert System (NIDES) A Summary," Computer Science Laboratory, SRI-CSL-95-07, May 1995 (*"Network NIDES"*);
- Y. Frank Jou et al., "Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure," Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, April 1997 (*"JiNao Report"*);
- Y. Frank Jou and S. Felix Wu, "Scalable Intrusion Detection for the Emerging Network Infrastructure, IDS Program Review," SRI, July 1997 (*"JiNao Slides"*);
- L. Todd Heberlein et al., "A Network Security Monitor," Proc. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 296-304, May 1990 (*"NSM 1990"*);
- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "Internetwork Security Monitor," Proc. of the 15<sup>th</sup> National Computer Security Conference, pp. 262-271, October 1992 (*"ISM 1992"*);
- B. Mukherjee, L.T. Heberlein, K.N. Levitt, "Network Intrusion Detection," IEEE Network, Vol. 8 No. 3, pp. 26-41, June 1994 (*"NID 1994"*);
- Steven R. Snapp et al., "Intrusion Detection Systems (IDS): A Survey of

Existing Systems and a Proposed Distributed IDS Architecture,” CSE-91-7, Feb. 1991 (“*DIDS Feb. 1991*”);

- Steven R. Snapp et al., “DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype,” Proc. 14<sup>th</sup> National Computer Security Conference, pp. 167-173, October 1991 (“*DIDS Oct. 1991*”);
- S. Staniford-Chen et al., “GrIDS – A Graph Based Intrusion Detection System for Large Networks,” 19<sup>th</sup> National Information Systems Security Conference, pp. 361-370, October 1996 (“*GrIDS 1996*”);
- Steven Cheung et al., “The Design of GRIDS: A Graph-Based Intrusion Detection System,” Technical Report, UC Davis Department of Computer Science, Davis California, May 14, 1997 (“*GrIDS 1997*”);
- Frank Edward Feather, “Fault Detection in an Ethernet Network via Anomaly Detectors,” Ph.D. thesis, Carnegie Mellon University, May, 1992 (“*Feather Thesis*”);
- “HP OpenView for Windows User Guide for Transcend Management Software, Version 6.1 for Windows and ‘97 for Windows NT,” 3Com, October 1997 (“*HP OpenView for Windows User Guide*”);
- “NetStalker, Installation and User’s Guide, Version 1.0.2” (May 1996);
- “RealSecure Release 1.0 for Windows NT 4.0 A User’s Guide and Reference Manual”;
- “NetRanger User’s Guide Version 1.3.1,” WheelGroup Corporation, 1997 (“*NetRanger Manual*”);
- U.S. Pat. No. 5,825,750, to Horace C. Thompson, entitled “Method and apparatus for maintaining security in a packetized data communications network,” filed on March 29, 1996 and issued on October 20, 1998 (“*the ’750 patent*”).

12. Whether the following systems or products were known or used before the inventions claimed, or were in public use or on sale prior to November 9, 1997:

- Network Security Monitor (“NSM”);
- Distributed Intrusion Detection System (“DIDS”);
- Graph-based Intrusion Detection System (“GrIDS”);
- NetRanger;
- ISS RealSecure;
- HP OpenView;
- NetStalker.

13. Whether, by clear and convincing evidence, ISS can prove that the above-listed printed publications, patents, systems or products satisfy each and every limitation of the asserted ISS claims of the '338, '203, '615 and '212 patents, either explicitly or inherently.

**B. Obviousness**

The anticipatory references listed above, as well as additional references relied upon in ISS's expert reports and disclosed on ISS's 35 U.S.C. § 282 filings will be referred to herein as "obviousness references."

14. Whether certain obviousness references are prior art under 35 U.S.C. § 102 (a), (b) or (e).
15. The level of ordinary skill in the art of intrusion detection / cyber security at the time of the invention of the '338, '203, '615 and '212 patents.
16. Whether, by clear and convincing evidence, ISS can prove that it would have been obvious to one of ordinary skill in the art of intrusion detection / cyber security at the time of the invention to combine certain obviousness references resulting in satisfaction of the limitations of the asserted ISS claims of the '338, '203, '615 and '212 patents.
17. Whether, by clear and convincing evidence, ISS can prove that it would have been obvious to one of ordinary skill in the art of intrusion detection / cyber security at the time of the invention to modify certain obviousness references resulting in satisfaction of the limitations of the asserted ISS claims of the '338, '203, '615 and '212 patents.
18. Whether there is any objective evidence of nonobviousness for any asserted patent claim, and whether SRI can prove a connection between any such objective evidence and the inventions of the asserted claims.

**C. Best Mode**

19. Whether, by clear and convincing evidence, ISS can prove that the common patent specification fails to disclose the best mode of practicing the asserted ISS claims of the

‘338, ‘203, ‘615 and ‘212 patents.

**D. Enablement**

20. Whether, by clear and convincing evidence, ISS can prove that one of ordinary skill in the art of intrusion detection / cyber security as of the priority date of the patents would have been unable to make and use the inventions described in the asserted ISS claims of the ‘338, ‘203, ‘615 and ‘212 patents without undue experimentation.

**E. Written Description**

21. Whether, by clear and convincing evidence, ISS can prove that the common patent specification fails to describe to one of ordinary skill in the art of intrusion detection / cyber security each and every limitation of the asserted ISS claims of the ‘338, ‘203, ‘615 and ‘212 patents.

**F. Indefiniteness**

22. Whether, by clear and convincing evidence, ISS can prove that the language of the asserted ISS claims of the ‘338, ‘203, ‘615 and ‘212 patents fails to particularly point out and distinctly claim the subject matter that the applicants regarded as their invention.

**IV. UNENFORCEABILITY**

23. Whether individuals associated with the filing or prosecution of the ‘338, ‘203, ‘615 and ‘212 patents either withheld information from the United States Patent & Trademark Office (the “PTO”) or misrepresented information to the PTO.

24. Whether, by clear and convincing evidence, ISS can prove that the withheld or misrepresented information was material.

25. Whether, by clear and convincing evidence, ISS can prove that the information was withheld or misrepresented with the intent to mislead or deceive the PTO.